



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/583,452	05/30/2000	Daniel R. Zaharris	M-8376-US	1693

7590 10/14/2005

MACPHERSON KWOK CHEN & HEID LLP  
1762 Technology Drive  
Suite 226  
San Jose, CA 95110

EXAMINER
----------

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 10/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/583,452

Applicant(s)

ZAHARRIS ET AL.

Examiner

Abdulhakim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 04 August 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1, 2 and 6-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 2, 6-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Response to Arguments***

1. This communication is in response to applicants' response received on August 04, 2005.
2. Amendments of the claims 1 and 20 and cancellation of claims 2 and 3 are acknowledged.
3. Applicant's arguments have been fully considered but they are not persuasive.
4. With regards to independent claims 1, 14 and 20, on pages 7 and 8 of remarks, applicants argue: In sharp contrast, claim 1 recites the act of "generating an internal key within the data storage engine using a pseudo-random number generator." (dependent claim 3 was cancelled and its limitation added to claim 1 to highlight the storage-engine-based nature of the digital rights management being recited in claim 1). Thus, the generation act has nothing to do with reading data from the disk.

In response to above argument, Bell discloses the use of a player-recorder (corresponding to the recited data storage engine) to generate a plurality of media keys (corresponding to the recited internal key(s)) based on a scheme that randomly generates numbers that is functionally equivalent to a pseudo-random number generator (see, for example, col. 8, line 59-col.9, line 3). A pseudo-random number generator is a device that uses an algorithm to generate a random number. Thus, act of "generating an internal key within the data storage engine using a pseudo-random number generator" is being performed by the system of Bell.

Art Unit: 2132

5. In light of the above submission the previous rejection of claims with taking into account the amendments of claims 1 and 20 is maintained.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**Claims 1, 2, 6, 8, 9, 14, 16, 17, 19 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Bell et al. (6,832,319 B1) (hereinafter Bell).**

1. Referring to claim 1, Bell discloses:

a method for copying electronic data, once only, on a storage medium that includes a medium ID and media key block (abstract; col. 2, lines 40-55) and Bell further discloses:

generating an internal key within the data storage engine using a pseudo-random number generator (Figs. 3 and 6; col. 7, lines 23-33; col. 8, line 59-col.9, line 3, where the media key corresponds to the recited internal key and the player-recorder corresponds to the recited data storage engine);

generating a combination key by combining a medium key with the internal key within the data storage engine (Figs. 3 and 6; col. 7, lines 23-33, where the media identification corresponds to the recited medium key and the content key corresponds to the recited combination key which is generated within the player); and

within the data storage engine, decrypting a first portion of data stored on the storage medium with said combination key (Figs. 3 and 6; col. 7, lines 23-33, where the content key corresponds to the recited combination key and it is used to decrypt the data read from the storage medium within the player).

2. Referring to claim 2, Bell discloses:

decrypting a master media key; and generating the medium key from the master media key (col. 9, lines 8-12, where medium key block corresponds to the recited master media key).

3. Referring to claim 6, Bell discloses:

The method of claim 1, wherein the combination key is generated by combining the internal key with the medium key in an exclusive OR function (col. 7, lines 59-62; col. 9, line 12-16).

4. Referring to claim 8, Bell discloses:

The method of claim 2 wherein the medium key comprises a mastered system area key, a writable system area key and a file system information key (Fig. 3; col. 6, lines 15-21).

5. Referring to claim 9, Bell discloses:

generating an additional internal key (col. 3, lines 25-50).

6. Referring to claims 14 and 20, Bell discloses:

Generating a plurality of internal keys using a pseudo-random number generator (data storage engine) (see col. 3, lines 17-50; col. 8, line 59-col. 9, line 16);

Decrypting a master media key and a file system structure corresponding to a first portion of the data using at least one internal key (see col. 7, lines 23-33; col. 9, lines 8-12, where medium key block corresponds to the recited master media key);

Generating a plurality of medium keys from the master media key (see col. 3, lines 17-50; col. 8, lines 46-67);

Generating a plurality of combination keys from the plurality of medium keys and the plurality of internal keys (see col. 4, lines 1-25; col. 7, lines 23-33, where the media identification corresponds to the recited medium key and the content key corresponds to the recited combination key which is generated within the player); and

Decrypting a first portion of the data using a first combination key (see col. 3, lines 25-30; col. 7, lines 23-33, where the content key corresponds to the recited

Art Unit: 2132

combination key and it is used to decrypt the data read from the storage medium within the player).

Encrypting a portion of data using said first combination key and storing the first portion on the storage medium (see col. 2, lines 50-55; col. 3, lines 8-16; col. 4, lines 1-8).

7. Referring to claims 16, 17 and 19, Bell discloses that DVD disk may contain different encrypted data recorded in different area of the disk each section with its own associated key that is used for the encryption of data and the combination key for decryption (see, for example, col. 3, lines 25-50; col. 5, lines 33-53; col. 8, lines 38-67).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 7, 10-13, 15, 18 and 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bell et al. (6,832,319 B1; hereinafter Bell) in view of Silverbrook et al. (6,334,190 B1; Silverbrook).**

1. Referring to claims 7, 18 and 21, Bell discloses that different data may be recorded on different area of a DVD disk and each portion of data encrypted and decrypted with particular keys using any type of cryptography technology (see, for example, col. 3, lines 25-50; col. 5, lines 33-53; col. 8, lines 38-67). But Bell does not expressly disclose the use of DES and triple DES for decryption and encryption.

Silverbrook discloses the use of DES standard for encryption and decryption (col. 3, lines 64-67) and specifically the use of triple DES for more security (col. 4, lines 7-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to utilize triple DES for encryption and decryption instead of single DES as taught in Silverbrook in the system of Angelo, because it would provide a much higher level of protection and security for the secure data (col. 1, lines 25-31).

2. Referring to claims 10, 11 and 13, these claims are rejected as applied to the like elements of claims 1, 4, 6 and 9 as stated above.

3. Referring to claim 12, Bell discloses any number of different encrypted data can be recorded on the DVD disk (see, for example, col. 3, lines 25-50; col. 5, lines 33-53; col. 8, lines 38-67) and any cryptosystem type and encryption key can be applied to the recorded information (col. 1, lines 56-64).



4. Referring to claim 15, Bell does not expressly disclose the use of a pseudo-random number generator comprising a logical feedback shift register (LFSR) and a seed for the LFSR. Silverbrook teaches the use of a pseudo-random number generator having LSFR (col. 11, line 60col. 12, line 15) to generate encryption keys. Silverbrook further teaches the use of a specific seed by the pseudo-random number generator (col. 4, line 7-col. 8, line 10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to utilize a LFSR pseudo-random number generator that uses a seed value as taught in Silverbrook in the system of Angelo, because it would provide a much higher level of protection for the secure data (col. 1, lines 25-31).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar  
Examiner  
Art Unit 2132 *A.N.*

October 11, 2005

*Gilberto Barron*  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100